UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/686,343	10/14/2003	Ernie Brickell	42P15784	7197

45209 7590 11/30/2009

INTEL/BSTZ
BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER	
TRUVAN, LEYNNA THANH	
ART UNIT	**PAPER NUMBER**
2435	
MAIL DATE	**DELIVERY MODE**
11/30/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/686,343
Filing Date: October 14, 2003
Appellant(s): BRICKELL ET AL.

Justin Brask
Blakely, Sokloff, Taylor & Zafman LLP

For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 8/13/2009 appealing from the Office action mailed 12/23/2008.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is substantially correct. The changes are as follows:

During the Final Office Action claims 1-2, 4-10, 12-18, and 20 was rejected under 35 U.S.C. 112, 1st paragraph, are now withdrawn.

To further clarify the decision in withdrawing the 112, 1st paragraph rejection for claimed feature "wherein the delegated environment is an environment to which the master owner token is not communicated". The claimed invention is broadly given in

accordance with the specification for the description is written. The specification states the environment controls a token (master or delegate) if that environment is the only environment that is given access to that token. The token of delegated environment can be given as belonging to a particular environment that is acknowledged or authorized access in that environment. The token can be master or it can be delegate token. Since the specification gives the option of either the master or the delegate token is controlled if that environment is the only environment that is given access to that token. So the delegate is controlled only in its environment, no mentioning of the master token in the delegate's token environment. Vice versa when choosing to give weight on the master token instead of the delegate. With this in mind, the description is silent on that the master token is not communicated to the delegate's environment since the description states that is the "only environment that is given access to that (delegate) token". Accordingly, in light of the specification the claimed master token is not communicated is given the interpretation according to Appellant.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

7,350,204	LAMBERT, ET AL.	3-2008
7,194,762	CHALLENER, ET AL.	3-2007

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-2, 4-10, 12-18, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable by Lambert, et al. (US 7,134,138), in view of Challener, et al. (US 7,194,762).

As per claim 1:

Lambert discloses a method of managing authorization tokens within a computer system comprising:

creating a master owner token indicating a management environment has full ownership *[of a trusted platform module]* within the computer system; (col.7, lines 55-57)

creating a delegate owner token for a delegated environment (col.8, lines 10-26 and 40-67 and col.22, lines 40- 45), wherein the delegated environment is an environment to which the master owner token is not communicated; (col.4, lines 6-17 and col.14, line 46 – col.15, line 20)

communicating the delegate owner token, to the delegated environment; and (col.9, lines 5-15 and col.22, lines 46-50)

allowing the delegated environment access *[to the trusted platform module]* when the delegated environment presents the delegate owner token to the *[trusted platform module]*. (col.3, line 66 - col.4, line 5 and col.11, lines 5-35)

Lambert discloses the claimed master owner token as the parent or normal access token that have the ownership or privileges that a restricted token does not. The claimed delegate owner token is given as a restricted token that have restricted access or privileges removed relative to its parent token (col.4, lines 5-15 and col.7, lines 54-57). Lambert explains the restricted token is derived from a parent token comprises a reduced subset of access rights/privileges relative to its parent token by altering (lessening) the access rights (col.8, lines 40-67). Lambert discloses the restricted access token have restrictions which have certain rights or privileges to determine whether software can run and the executing environment in which it will run (col.3, line 66 - col.4, line 18). This shows the restricted token is associated with each process which is the claimed environment and enables restricting actions by possibly executable software content (col.9, lines 5-15 and col.11, lines 5-35). Lambert also discusses returning a token to associate with a file to the software function where if a token is returned, it may be the parent token (unchanged) if no restricted execution environment is required by the rule or a restricted token that establishes a restricted execution environment/context for the processes of the software file (col.16, lines 9-24). Thus, Lambert does not suggest the parent token is communicated to the delegated environment since the focus is the restricted token that is associated to a process/software. Hence,

Lambert reads on the claimed creating a delegate owner token for a delegated environment wherein the delegated environment is an environment to which the master owner token is not communicated. However, Lambert did not include a TPM.

Challener discloses a method and system for improved security password-based access to computer networks. The system comprises a server where the server comprises a security chip (col.2, lines 45-49). The invention comprises a security chip, such as a Trusted Platform Module (TPM) where a phrase is signed by the security chip using an encryption key assigned either to the remote user or the security chip (col.2, lines 16-18 and 28-32). The security chip comprises encryption keys, such as a public key/private key pair assigned to the chip (col.2, lines 51-53). Challener discloses a remote user request access to the computer network by providing an ID and password to the server (col.3, lines 4-7). The password is according to the remote user and for access to the server. Challener discloses the system comprising a server (delegated environment) and the remote user password (delegate owner token) where the user's password is given to the server and to the security chip (TPM), rather than the master token being given to the server (col.4, lines 57-59). Further, Challener teaches using a security chip further decreases the exposure to brute force attacks and such TPM allow only certain number of unsuccessful entries of a password before a user is locked (col.3, lines 24-26). So the user of the security chip enforces protection against hardware hammering (col.4, lines 15-19).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teachings of Lambert with Challener to teach of a trusted platform module (TPM) because using a security chip decrease the exposure to brute force attacks and enforces protection against hardware hammering (Challener - col.3, lines 24-26 and col.4, lines 18-19).

As per claim 2: See Lambert on col.7, lines 26-55; discloses the method of claim 1, further comprising storing the master owner token in a secure storage within the computer system.

As per claim 4: See Lambert on col.8, lines 10-26 and 40-67 and col.22, lines 40- 45; discloses the method of claim 1, wherein creating the delegate owner token comprises the management environment sealing the delegate owner token to the delegated environment.

As per claim 5: See Lambert on col.4, lines 5-15 and col.8, lines 40-67; discloses the method of claim 1, further comprising wherein the master owner token indicating the management environment can change at least one of the master owner token and a delegate owner token.

As per claim 6: See Lambert on col.9, lines 5-15 and col.11, lines 5-35; discloses the method of claim 1, further comprising launching the management environment and then launching the delegated environment.

As per claim 7: See Lambert on col.9, lines 36-67; discloses the method of claim 1, further comprising storing the delegate owner token in an access control list in the resource.

As per claim 8: See Lambert on col.9, lines 36-67 and col.10, lines 20-33; discloses the method of claim 7, further comprising removing, by the management environment, the delegate owner token from the access control list and adding a different delegate owner token to the access control list.

As per claim 9:

Lambert discloses an article comprising:

a storage medium having a plurality of machine readable instructions, wherein when the instructions are executed by a processor, the instructions provide for managing authorization tokens within a computer system by creating a master owner token indicating an administrative environment has full ownership *[of a trusted platform module]* within the computer system; (col.6, lines 1-37 and col.7, lines 55-57)

creating a delegate owner token for a delegate environment (col.8, lines 10-26 and 40-67 and col.22, lines 40- 45), wherein the delegated environment is an environment to which the master owner token is not communicated; (col.4, lines 6-17 and col.14, line 46 – col.15, line 20)

communicating the delegate owner token to the delegated environment; and (col.9, lines 5-15 and col.22, lines 46-50)

allowing the delegated environment access *[to the trusted platform module]* when the delegated environment presents the delegate owner token *[to the trusted platform module].* (col.3, line 66 - col.4, line 5 and col.11, lines 5-35)

Lambert discloses the claimed master owner token as the parent or normal access token that have the ownership or privileges that a restricted token does not. The claimed delegate owner token is given as a restricted token that have restricted access or privileges removed relative to its parent token (col.4, lines 5-15 and col.7, lines 54-57). Lambert explains the restricted token is derived from a parent token comprises a reduced subset of access rights/privileges relative to its parent token by altering (lessening) the access rights (col.8, lines 40-67). Lambert discloses the restricted access token have restrictions which have certain rights or privileges to determine whether software can run and the executing environment in which it will run (col.3, line 66 - col.4, line 18). This shows the restricted token is associated with each process which is the claimed environment and enables restricting actions by possibly executable software content (col.9, lines 5-15 and col.11, lines 5-35). Thus, Lambert does not suggest the parent token is communicated to the delegated environment since the focus is the restricted token that is associated to a process/software. Hence, Lambert reads on the claimed creating a delegate owner token for a delegated environment wherein the delegated environment is an environment to which the master owner token is not communicated. However, Lambert did not include a TPM.

Challener discloses a method and system for improved security password-based access to computer networks. The system comprises a server where the server comprises a security chip (col.2, lines 45-49). The invention comprises a security chip, such as a Trusted Platform Module (TPM) where a phrase is signed

by the security chip using an encryption key assigned either to the remote user or the security chip (col.2, lines 16-18 and 28-32). The security chip comprises encryption keys, such as a public key/private key pair assigned to the chip (col.2, lines 51-53). Challener discloses a remote user request access to the computer network by providing an ID and password to the server (col.3, lines 4-7). The password is according to the remote user and for access to the server. Challener discloses the system comprising a server (delegated environment) and the remote user password (delegate owner token) where the user's password is given to the server and to the security chip (TPM), rather than the master token being given to the server (col.4, lines 57-59). Further, Challener teaches using a security chip further decreases the exposure to brute force attacks and such TPM allow only certain number of unsuccessful entries of a password before a user is locked (col.3, lines 24-26). So the user of the security chip enforces protection against hardware hammering (col.4, lines 15-19).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teachings of Lambert with Challener to teach of a trusted platform module (TPM) because using a security chip decrease the exposure to brute force attacks and enforces protection against hardware hammering (Challener - col.3, lines 24-26 and col.4, lines 18-19).

As per claim 10: See Lambert on col.7, lines 26-55; discloses the article of claim 9, further comprising instructions for storing the master owner token in a secure storage within the computer system.

As per claim 12: See Lambert on col.8, lines 10-26 and 40-67 and col.22, lines 40- 45; discloses the article of claim 9, wherein creating the delegate owner token comprises the administrative environment sealing the delegate owner token to the delegated environment.

As per claim 13: See Lambert on col.4, lines 5-15 and col.8, lines 40-67; discloses the article of claim 9, further comprising the master owner token indicating the administrative environment can change at least one of the master owner token and the delegate owner token.

As per claim 14: See Lambert on col.9, lines 5-15 and col.11, lines 5-35; discloses the article of claim 9, further comprising instructions for launching the administrative environment and then launching the delegated environment.

As per claim 15: See Lambert on col.9, lines 36-67; discloses the article of claim 9, further comprising instructions for storing the delegate owner token in an access control list in the resource.

As per claim 16: See Lambert on col.9, lines 36-67 and col.10, lines 20-33; discloses the article of claim 9, further comprising instructions for removing, by the administrative environment, the delegate owner token from the access control list and adding a different delegate owner token to the access control list.

As per claim 17:

Lambert discloses a computer system comprising:

a plurality of delegated environments; (col.4, lines 1-4 and col.15, line 61 - col.16, line 24)

a management environment to create a master owner token indicating the management environment has full ownership *[of a trusted platform module]* within the computer system (col.7, lines 55-57), to create a plurality of delegate owner tokens indicating partial ownership (col.8, lines 10-26 and 40-67 and col.22, lines 40- 45) *[of the trusted platform module]*, and to communicate a selected one of the plurality of delegate owner tokens to a selected one of the plurality of delegated environments (col.9, lines 5-15 and col.22, lines 46-50), wherein the selected one of the plurality of delegated environment is an environment to which the master owner token is not communicated; (col.4, lines 6-17 and col.14, line 46 – col.15, line 20)

wherein *[the trusted platform module]* stores delegate owner tokens created by the management environment and allows the selected one of the plurality of delegated environments access *[to the trusted platform module]* when the selected one of the plurality of delegate owner tokens is presented *[to the trusted platform module]* by the selected one of the plurality of delegated environments. (col.3, line 66 - col.4, line 5 and col.11, lines 5-35)

Lambert discloses the claimed master owner token as the parent or normal access token that have the ownership or privileges that a restricted token does not. The claimed delegate owner token is given as a restricted token that have restricted access or privileges removed relative to its parent token (col.4, lines 5-15 and col.7, lines 54-57). Lambert explains the restricted token is derived from a parent token comprises a reduced subset of access rights/privileges relative to its

parent token by altering (lessening) the access rights (col.8, lines 40-67). Lambert discloses the restricted access token have restrictions which have certain rights or privileges to determine whether software can run and the executing environment in which it will run (col.3, line 66 - col.4, line 18). This shows the restricted token is associated with each process which is the claimed environment and enables restricting actions by possibly executable software content (col.9, lines 5-15 and col.11, lines 5-35). Thus, Lambert does not suggest the parent token is communicated to the delegated environment since the focus is the restricted token that is associated to a process/software. Hence, Lambert reads on the claimed creating a delegate owner token for a delegated environment wherein the delegated environment is an environment to which the master owner token is not communicated. However, Lambert did not include a TPM.

Challener discloses a method and system for improved security password-based access to computer networks. The system comprises a server where the server comprises a security chip (col.2, lines 45-49). The invention comprises a security chip, such as a Trusted Platform Module (TPM) where a phrase is signed by the security chip using an encryption key assigned either to the remote user or the security chip (col.2, lines 16-18 and 28-32). The security chip comprises encryption keys, such as a public key/private key pair assigned to the chip (col.2, lines 51-53). Challener discloses a remote user request access to the computer network by providing an ID and password to the server (col.3, lines 4-7). The password is according to the remote user and for access to the server. Challener

discloses the system comprising a server (delegated environment) and the remote user password (delegate owner token) where the user's password is given to the server and to the security chip (TPM), rather than the master token being given to the server (col.4, lines 57-59). Further, Challener teaches using a security chip further decreases the exposure to brute force attacks and such TPM allow only certain number of unsuccessful entries of a password before a user is locked (col.3, lines 24-26). So the user of the security chip enforces protection against hardware hammering (col.4, lines 15-19).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teachings of Lambert with Challener to teach of a trusted platform module (TPM) because using a security chip decrease the exposure to brute force attacks and enforces protection against hardware hammering (Challener - col.3, lines 24-26 and col.4, lines 18-19).

As per claim 18: See Lambert on col.7, lines 26-55; discloses a computer system of claim 17, further comprising a secure storage to store the master owner token.

As per claim 19: Cancelled

As per claim 20: See Lambert on col.9, lines 36-67 and col.10, lines 20-33; discloses the computer system of claim 19, wherein the trusted platform module comprises an access control list for storing the delegate owner tokens received from the management environment.

(10) Response to Argument

Claims 1-2, 4-10, 12-18 and 20 rejection under 35 U.S.C. § 112, 1st paragraph rejection:

Regarding the argument on pg.9-10, in the Final Office Action claims 1-2, 4-10, 12-18, and 20 was rejected under 35 U.S.C. 112, 1st paragraph, are now withdrawn.

To further clarify the decision in withdrawing the 112, 1st paragraph rejection for claimed feature "wherein the delegated environment is an environment to which the master owner token is not communicated". The claimed invention is broadly given in accordance with the specification for the description is written. The specification states the environment controls a token (master or delegate) if that environment is the only environment that is given access to that token. The token of delegated environment can be given as belonging to a particular environment that is acknowledged or authorized access in that environment. The token can be master or it can be delegate token. Since the specification gives the option of either the master or the delegate token is controlled if that environment is the only environment that is given access to that token. So the delegate is controlled only in its environment, no mentioning of the master token in the delegate's token environment. Vice versa when choosing to give weight on the master token instead of the delegate. With this in mind, the description is silent on that the master token is not communicated to the delegate's environment since the description states that is the "only environment that is given access to that (delegate) token". Accordingly, in light of the specification the claimed master token is not communicated is given the interpretation according to Appellant.

Claims 1-2, 4-10, 12-18,and 20 rejection under 35 U.S.C. §103(a)

Appellant addresses independent claims 1 and 9 from which claims 2, 4-8, 10, and 12-16 depend, include the feature, "the delegated environment is an environment to which the master owner token is not communicated". Independent claim 17, from which claims 18 and 20 depend, recites a similar feature.

In response to the argument (pg.11), Appellant finds the lack of suggestion is certainly not an explicit disclosure and the lack of suggestion in Lambert is also not an inherent disclosure that the parent token of Lambert is not communicated to the delegated environment because none of the technical features disclosed by Lambert would restrict the parent token of Lambert from being communicated to the delegated environment. This interpretation is in accordance with Appellant as discussed earlier in response to the 112, 1st paragraph rejection (now withdrawn). Thus, examiner has properly interpreted the claimed the master (parent) token is not communicated to the delegated environment according the description of the specification which was pointed out by Appellant.

As for prior art, Lambert suggests that the parent token (master token) is not communicated because it focuses on the access and privileges for restricted token that is able to be communicated for an execution environment in which it will run (col.4, lines 1-20). Lambert discusses returning a token to associate with a file to the software function where if a token is returned, it may be the parent token (unchanged) if no restricted execution environment is required by the rule or a restricted token that establishes a restricted execution environment/context for the processes of the software

file (col.16, lines 9-24). Lambert discloses a process may be associated with the restricted token such that when the process desires access to an object the process specifies the type of access it desire and the token is provided to the object manager. Figure 3 shows the token is the restricted token (col.9, lines 1-15). A process such as a process of a user or application requesting to open a software file has an access token associated with it (col.14, lines 46-49). Lambert discloses that the restricted token is only associated to a process which is in terms of an environment. Thus, Lambert suggests the restricted (delegate) token is not associated to the parent (master) token which obviously suggests that the parent (master) token is not associated (communicated) with the restricted token's process (environment). In addition, Lambert discloses a restricted token is associated with the software file whereby if creation of a process is requested for the software file, any process of the software file is restricted in its access rights and privileges according to the restricted token (col.15, lines 61-66). This show the software file is the only environment that is given access to that restricted token such that the software file controls the restricted token since the process or software file is restricted in its access rights and privileges. Therefore, Lambert reads onto the claimed invention and in accordance with the specification.

Regarding the argument on pg.12: Appellant finds that neither Lambert nor Challener disclosing "wherein the delegated environment is an environment to which the master owner token is not communicated". Challener is brought forth to modify Lambert's invention the teaching of a Trusted Platform Module. Challener discloses a method and system for improved security that includes a security chip,

such as a Trusted Platform Module (TPM) where a phrase is signed by the security chip using an encryption key assigned either to the remote user or the security chip (col.2, lines 16-18 and 28-32). Challener discloses the system comprising a server (delegated environment) and the remote user password (delegate owner token) where the user's password is given to the server and to the security chip (TPM), rather than the master token being given to the server (col.4, lines 57-59). Further, Challener teaches using a security chip further decreases the exposure to brute force attacks and such TPM allow only certain number of unsuccessful entries of a password before a user is locked (col.3, lines 24-26). So the user of the security chip enforces protection against hardware hammering (col.4, lines 15-19). Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teachings of Lambert with Challener to teach of a trusted platform module (TPM) because using a security chip decrease the exposure to brute force attacks and enforces protection against hardware hammering (Challener - col.3, lines 24-26 and col.4, lines 18-19). Accordingly, the Lambert and Challener combination reads on the current invention as claimed.

Accordingly, all dependent claims are also rejected by virtue of their pendency.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/L. T. T./

Examiner, Art Unit 2435

Conferees:

/Nirav B. Patel/

Patent Examiner, Art Unit 2435

/Kimyen Vu/

Supervisory Patent Examiner, Art Unit 2435